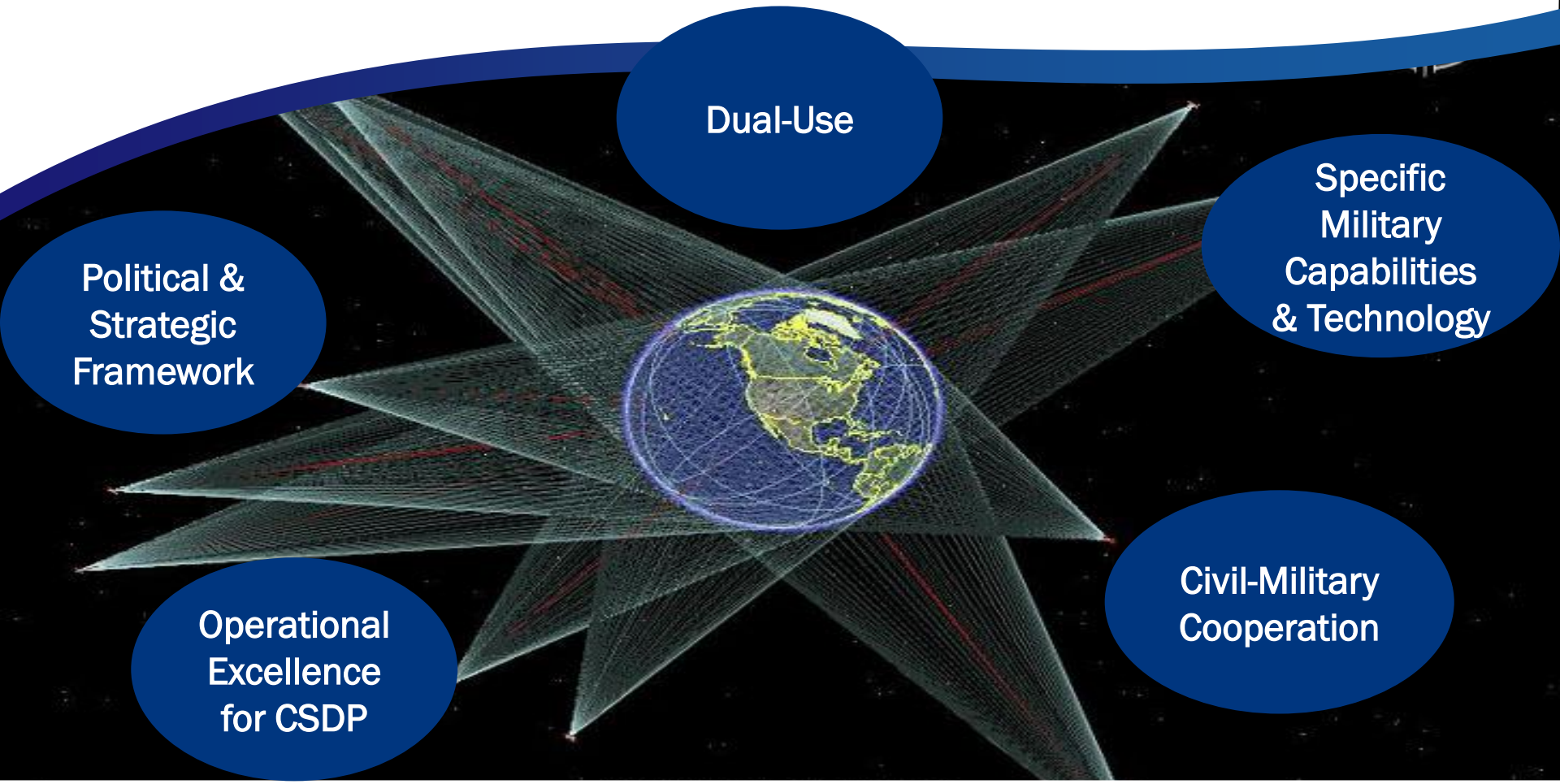
ENISA Workshop CTI – EU | Bonding EU Cyber Threat Intelligence
Rome, 30-31 October 2017
Wolfgang Roehrig
EDA Programme Manager Cyber Defence
Wolfgang.Roehrig@eda.europa.eu
+32 (0)2 504 2966

EUROPEAN DEFENCE AGENCY



Cyber Threat Intelligence Information Sharing for EU-led military Operations – Is the time ready now?

Talking Points

- EDA and Cyber Defence
- Cyber Defence and Cyber Threat Intelligence Considerations in the military Operations Planning Process
  - EDA „precursor“ work; Architecture and OPP
  - Cyber Situation Awareness;
  - CyTelOps
- The EU approach to Cyber Defences for EU-led Operations
  - The EU Cyber Defence Concept for military operations and missions
  - Considerations on Cyber Risk Management;
- Conclusions-Discussion Points

Talking Points

- EDA and Cyber Defence
- Cyber Defence and Cyber Threat Intelligence Considerations in the military Operations Planning Process
  - EDA „precursor“ work; Architecture and OPP
  - Cyber Situation Awareness;
  - CyTelOps
- The EU approach to Cyber Defences for EU-led Operations
  - The EU Cyber Defence Concept for military operations and missions
  - Considerations on Cyber Risk Management;
- Conclusions-Discussion Points

Mission

… to support
the Council and the Member States in their effort to improve the European Union's defence capabilities for the Common Security and Defence Policy.*

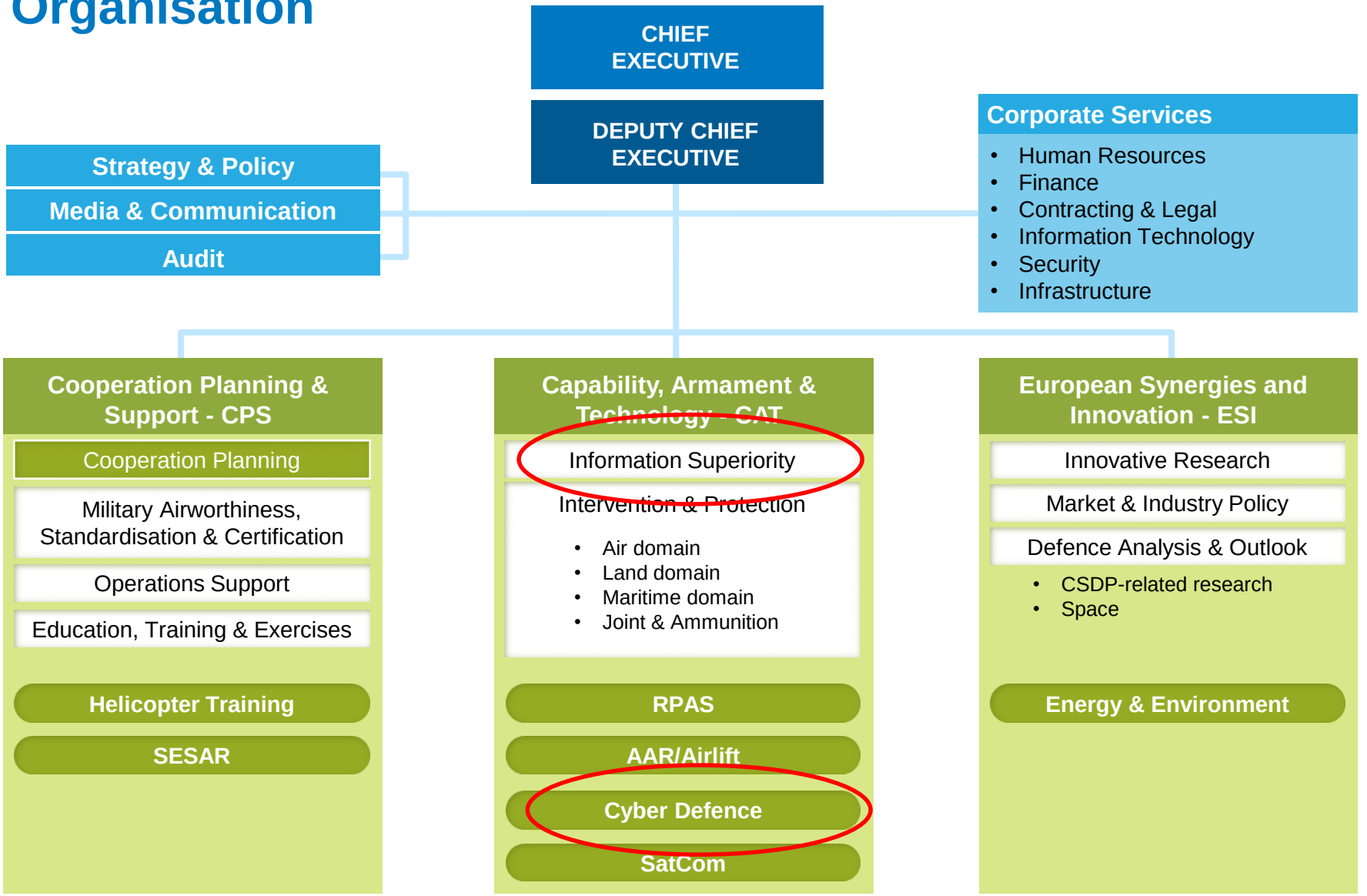
*Treaty of Lisbon, signed in 2007, entered into force in 2009

EUROPEAN DEFENCE AGENCY

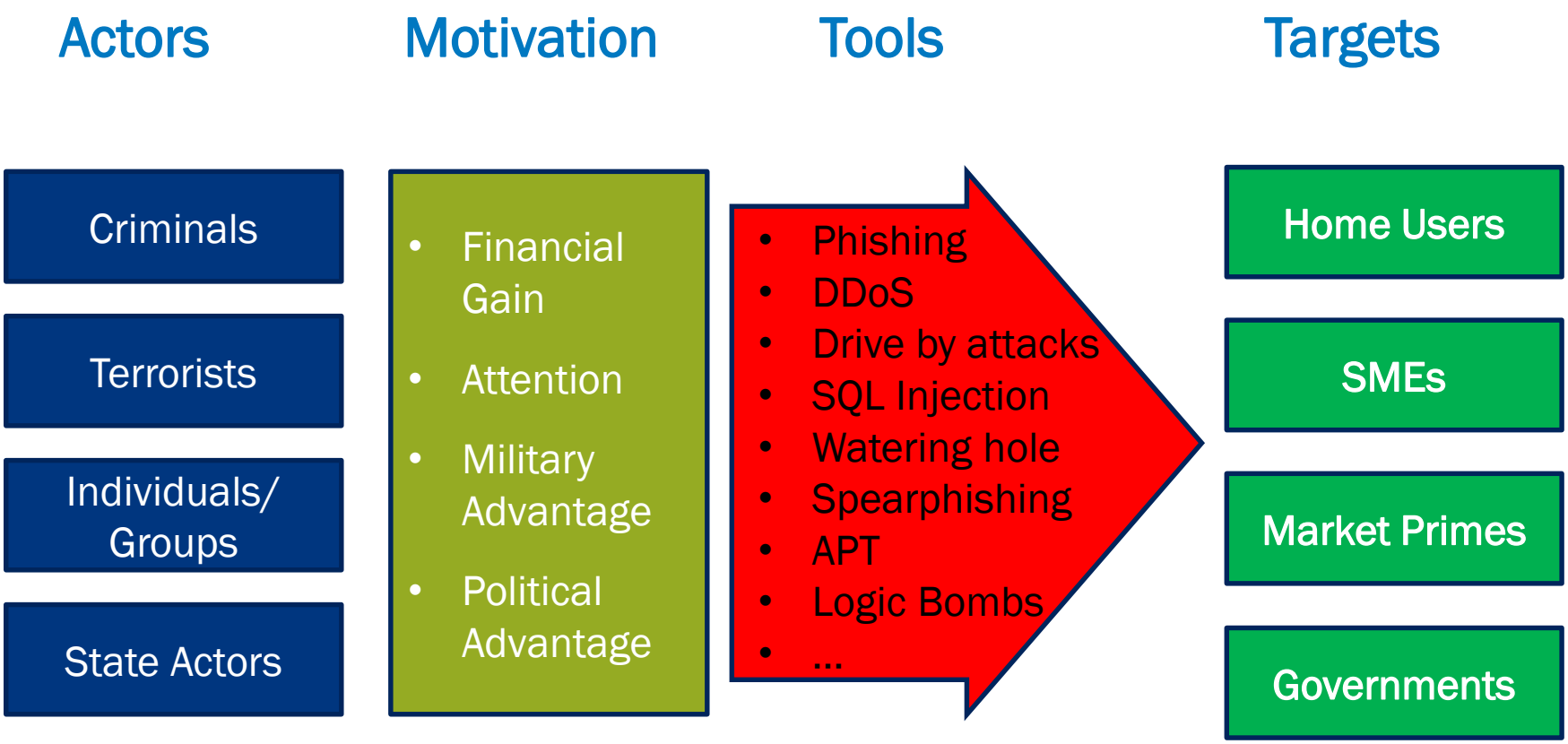
... so we do on Cyber Defence!

www.eda.europa.eu

Organisation



Cyber Threats; Who, Why, How?

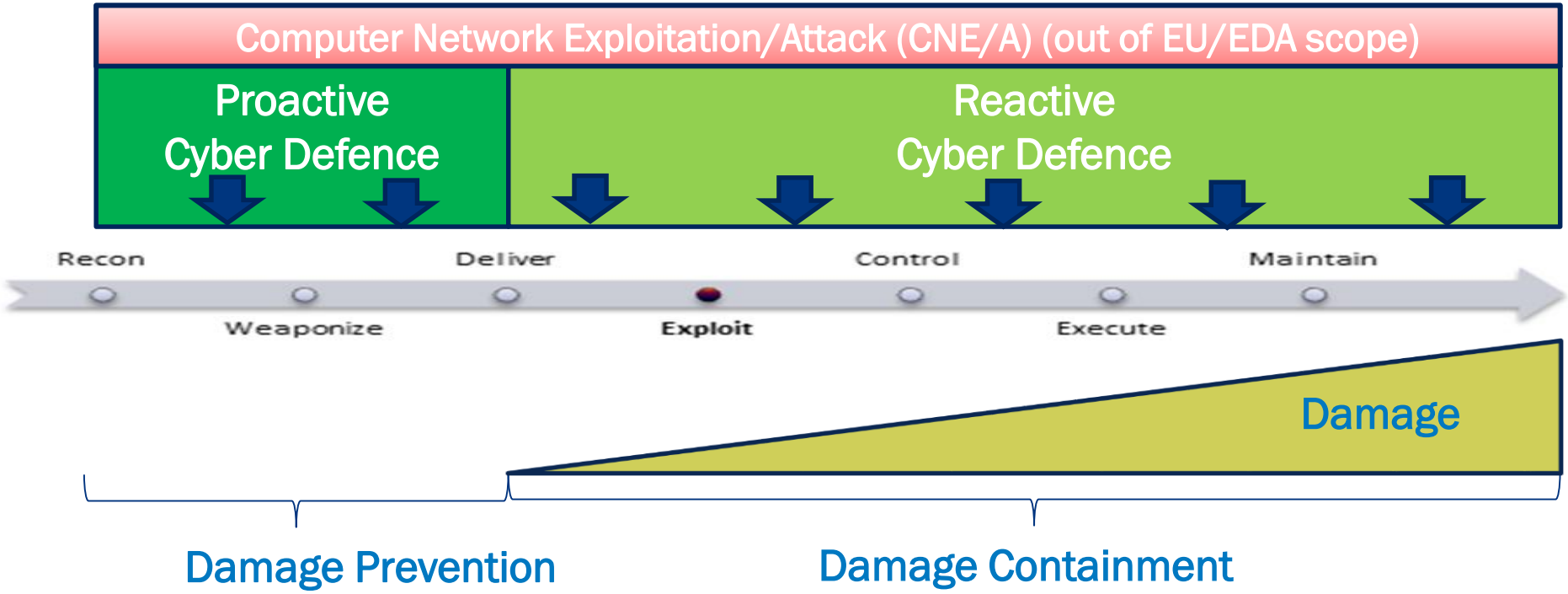


The Military Requirement - Attacker's "Kill Chain"

The military requirements on Cyber Defence capabilities for CSDP are to:

- prepare for, prevent,
- detect, respond to, recover from, and
- learn lessons from

attacks, damage or unauthorized access affecting information infrastructures … that support and enable the conduct of EU-led military tasks and operations.



Talking Points

- EDA and Cyber Defence
- Cyber Defence and Cyber Threat Intelligence Considerations in the military Operations Planning Process
  - EDA „precursor“ work; Architecture and OPP
  - Cyber Situation Awareness;
  - CyTelOps
- The EU approach to Cyber Defences for EU-led Operations
  - The EU Cyber Defence Concept for military operations and missions
  - Considerations on Cyber Risk Management;
- Conclusions-Discussion Points

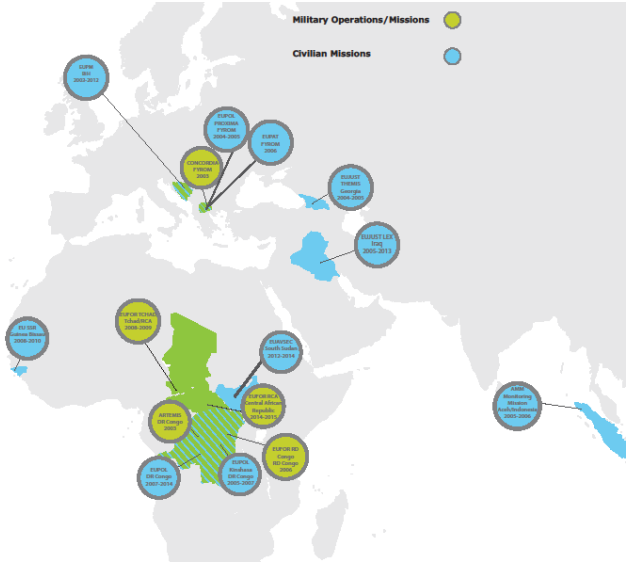
EU-led Crisis Management Operations and Missions

- "Petersberg Tasks" as expanded 2009 in the TEU Art. 42
  - humanitarian aid and rescue;
  - conflict prevention and peace-keeping;
  - tasks of combat forces in crisis management, including peacemaking;
  - joint disarmament operations;
  - military advice and assistance;
  - post-conflict stabilisation [and reconstruction].

Current EU-led operations and civil missions

- Military Operations & Missions
  - Training missions
  - Monitoring
  - …
- Civil Missions
  - Observer missions
  - Police Assistance
  - Legal Assistance
  - …

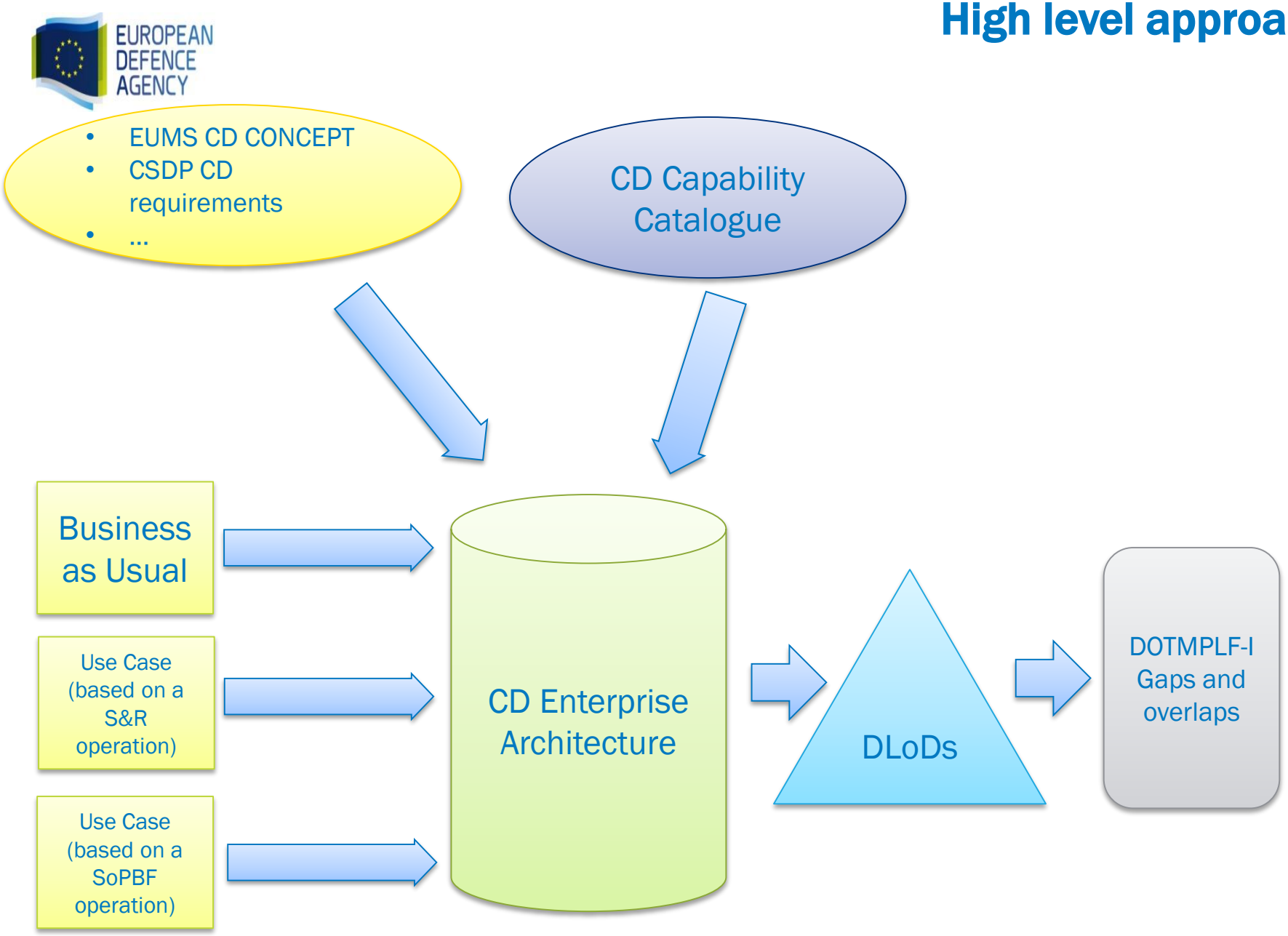
Completed EU-led operations and civil missions



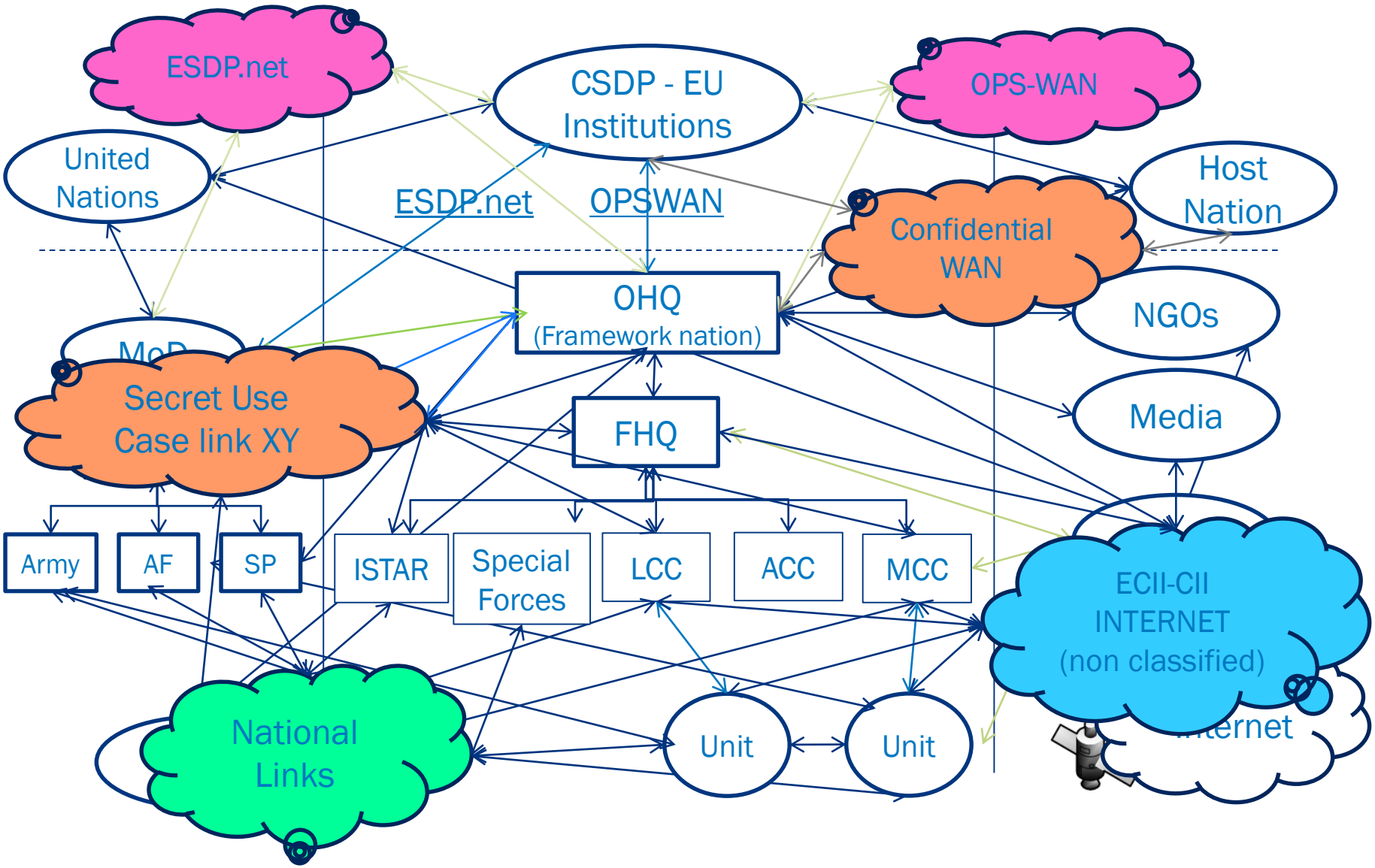
Cyber Risks & CDSP Military Operations

- Ever-growing **dependence on digitally-networked Information** to deliver military effects;
- Cyber Risks impinge on external, our **Civil Enabler** dependencies, as well as on our **Military Capabilities**;
- Successful adversaries' Cyber Attacks can result in **Mission difficulties, or even Mission failure**;
- **EU-led Military Operations** are, by their comprehensive/collaborative nature, **uniquely exposed to Cyber Risks**;
- Cyber Risk Management is inherently a **continuous process**, as adversaries continuously adapt their Attack Methods, and also our own Cyber posture changes over time;

High level approach



USE CASE Example



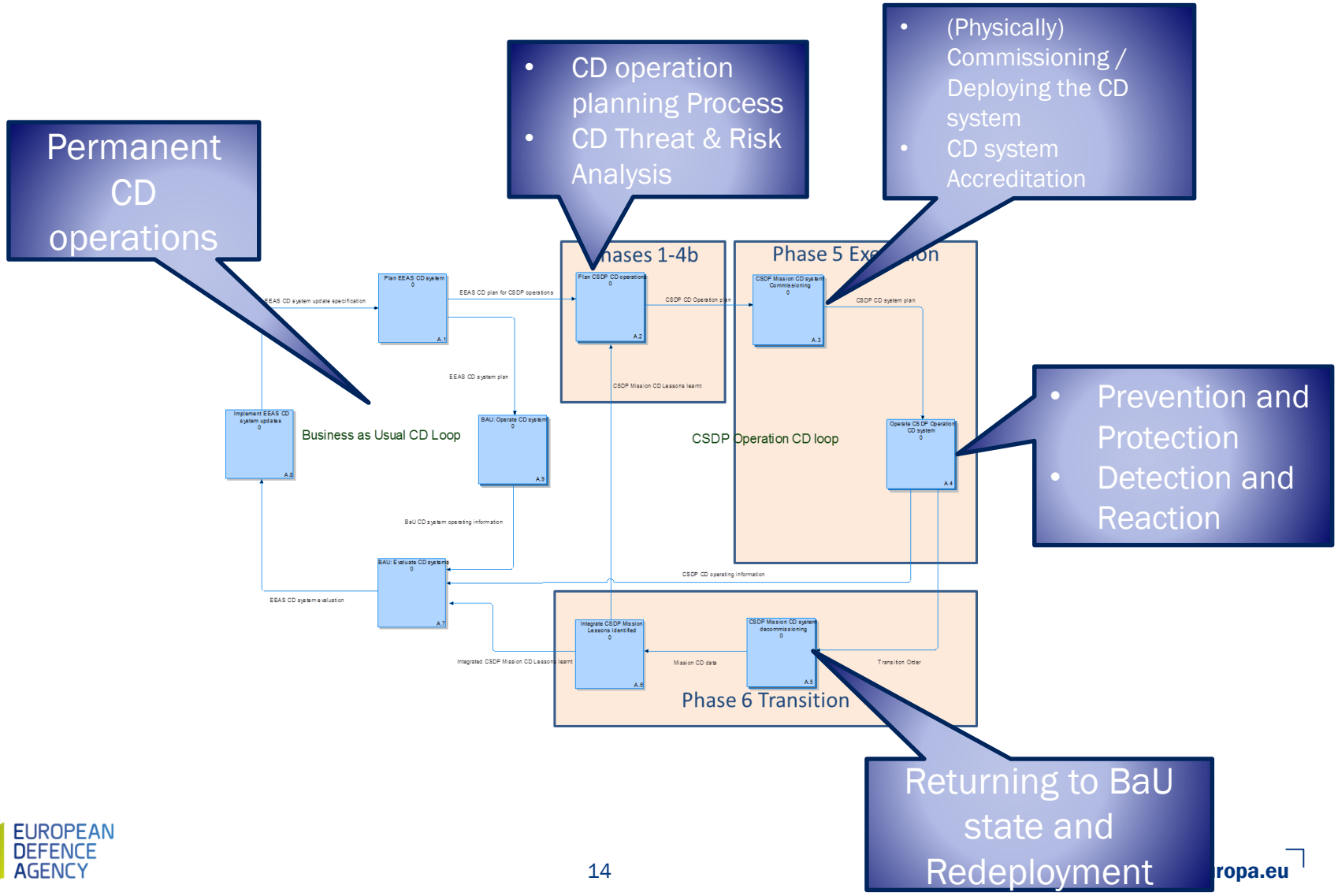
What can the CD EA tell us?

- How CD activities are connected to CD nodes and CD information flows: i.e. **what is done by whom;**

- How CD capabilities are connected to CD nodes and CD services: i.e. **what is needed by whom**, and

- Where the gaps are in doctrine, organisation, training, leadership, materiel, personnel and facilities.

Important cyber defence factors for each phase



The Operations Planning Process

PHASE 1 Initiation	PHASE 2 Operational Appreciation of the Strategic Environment	PHASE 3 Operational Estimate	PHASE 4 Operational Plan Development
• Realize a critical situation is emerging • Gathering and processing of information • Get a comprehensive understanding of the situation • Produce valid fundaments for decision making, pdating them and responding to decisions. • Operational Appreciation of the Strategic Environment	• Go even more into detail in understanding the nature of the problem and the objectives for any military response • Provide operational advice to the strategic level on strategic Military Response Options (MROs)	• Understand the problem, the operational environment and the mission itself. • Perform three analyses: o The Factor Analysis o The Center of Gravity Analysis o Risk Assessment. • Development of Courses of Action (COA).	• Development of the operational concept and plan. • Finalize the planning documents for distribution • Subordinate units that are tasked to execute the plan

CPOE
Comprehensive Preparation of Operational Environment


NATO UNCLASSIFIED

SUPREME HEADQUARTERS ALLIED POWER EUROPE
BELGIUM

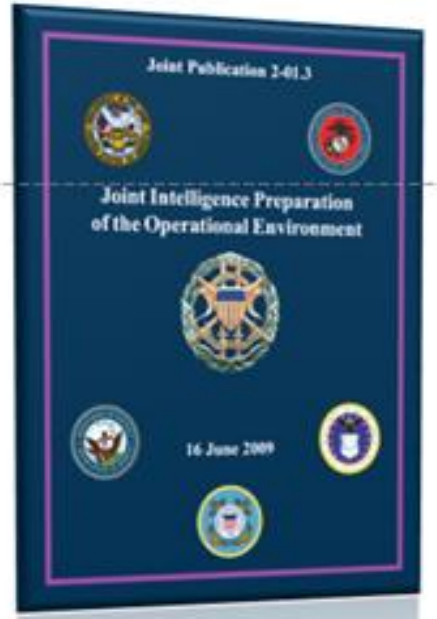
ALLIED COMMAND OPERATIONS
COMPREHENSIVE OPERATIONS
PLANNING DIRECTIVE
COPD INTERIM V1.0

17 DECEMBER 2010

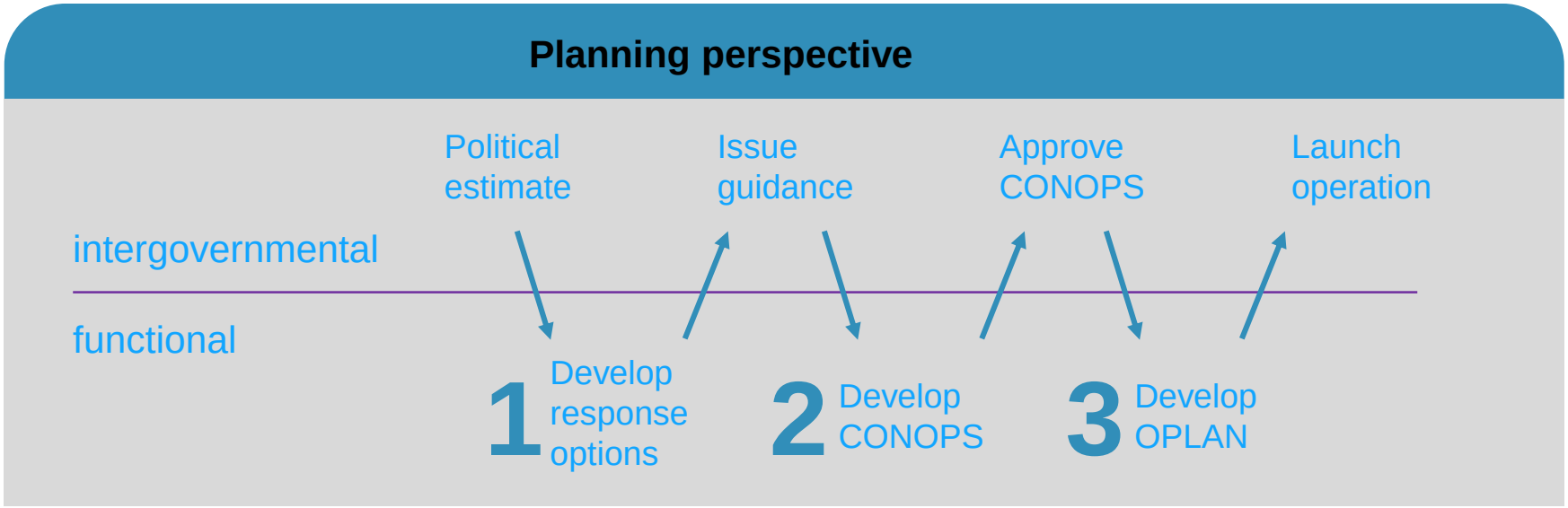
NATO UNCLASSIFIED

- Political
- Military
- Economics
- Social
- Information
- Infrastructure

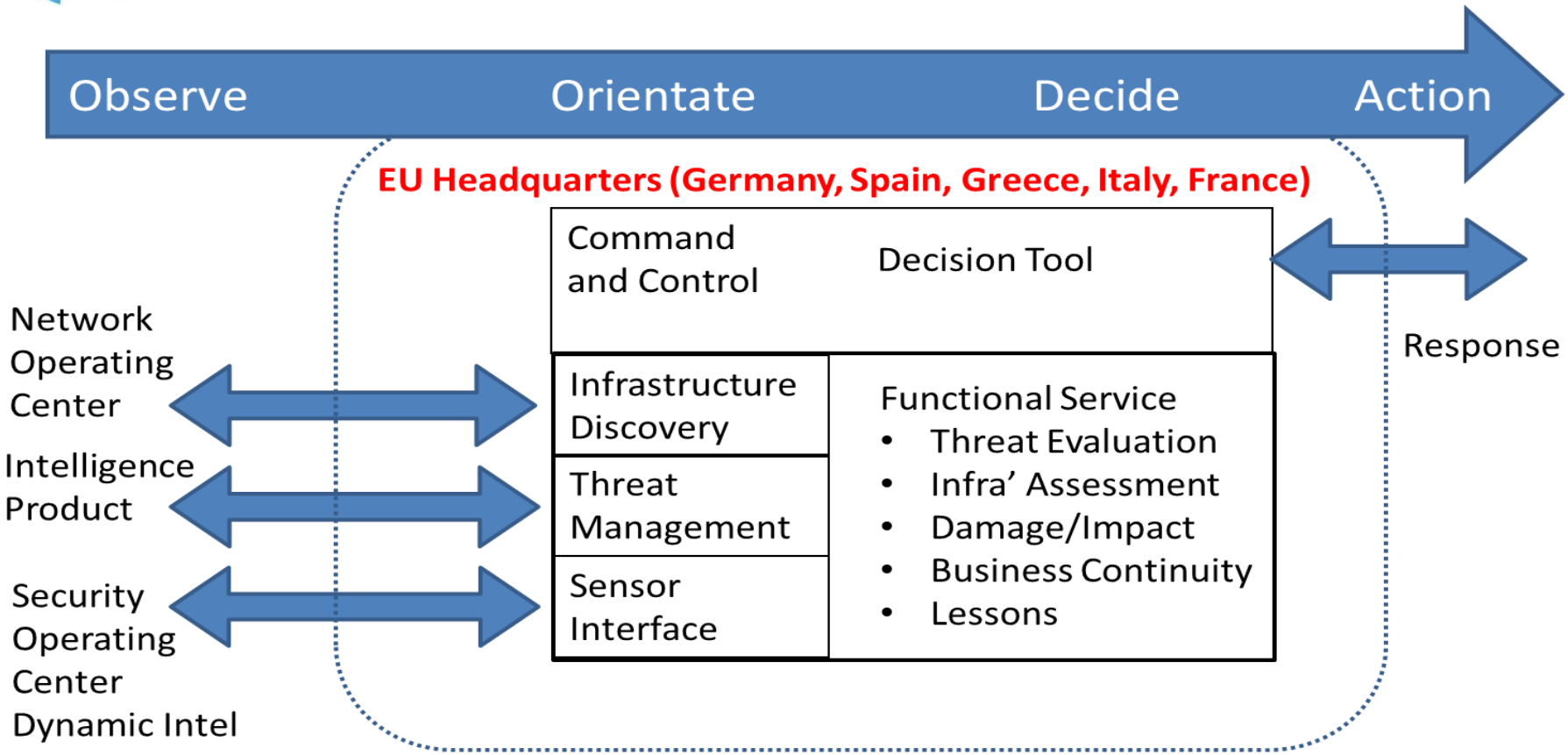
Cyber Factors



Operations Planning and Cyber Risk Management



Specific (military) Capabilities
« Cyber Situation Awareness Package »

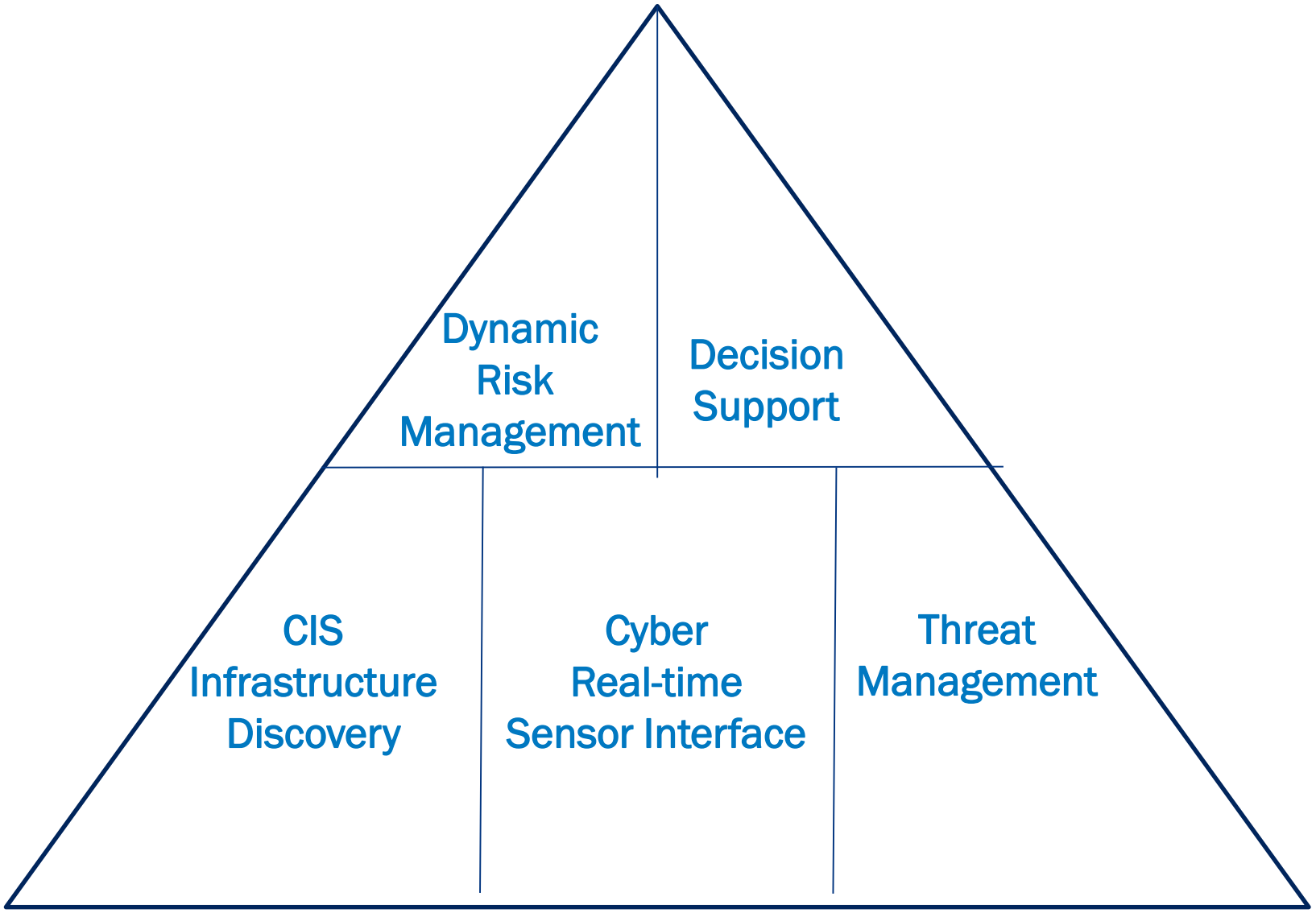


=> Well-informed Cyber decision-making.

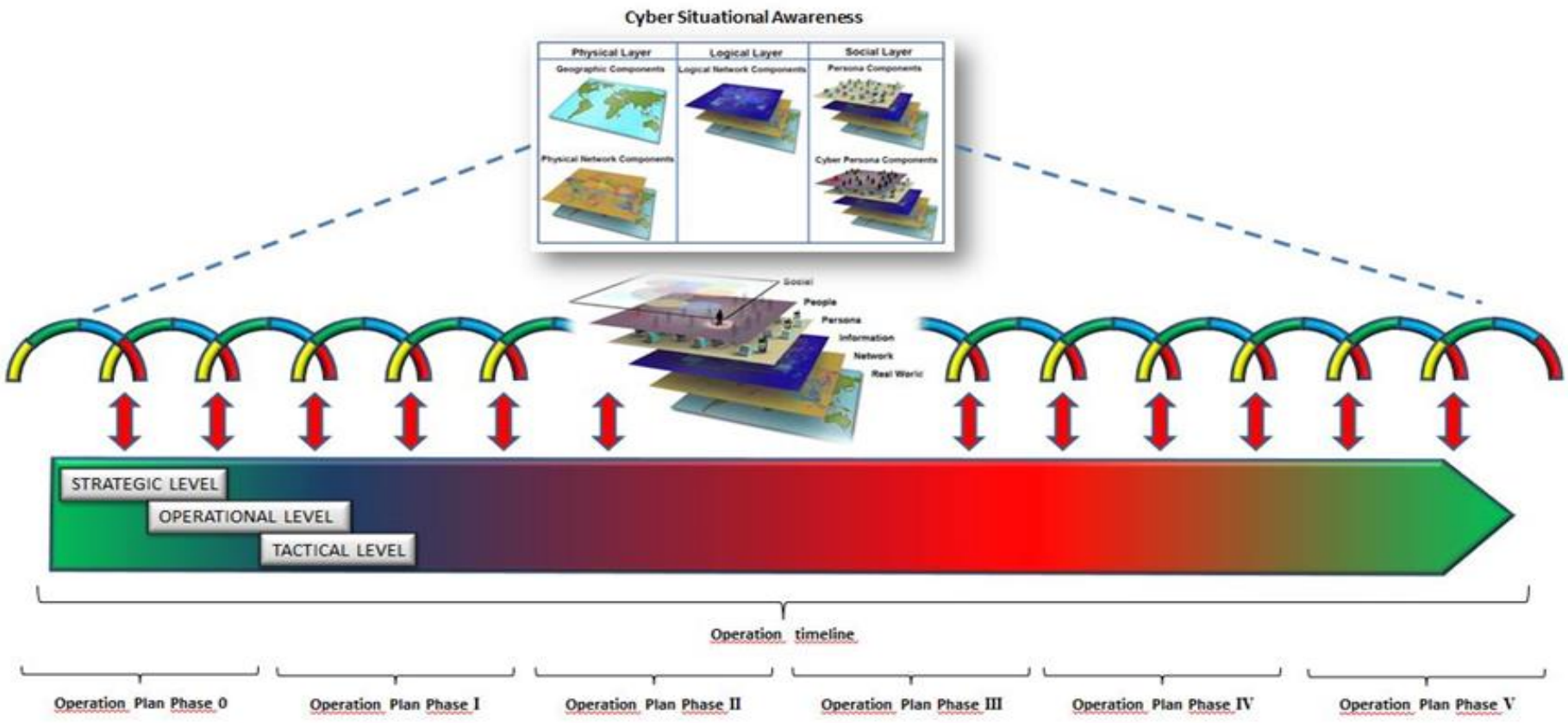
Start in 2013 with EDA initiative and Common Staff Target (CST) agreed mid 2014.
Common Staff Requirement (CSR) agreed in 2016. PA under negotiation

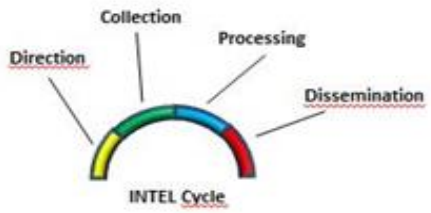
Contributing Member States: **DE, ES, IT**

Cyber Situation Awareness. Research Areas



Information & Intelligence Gathering Cycles



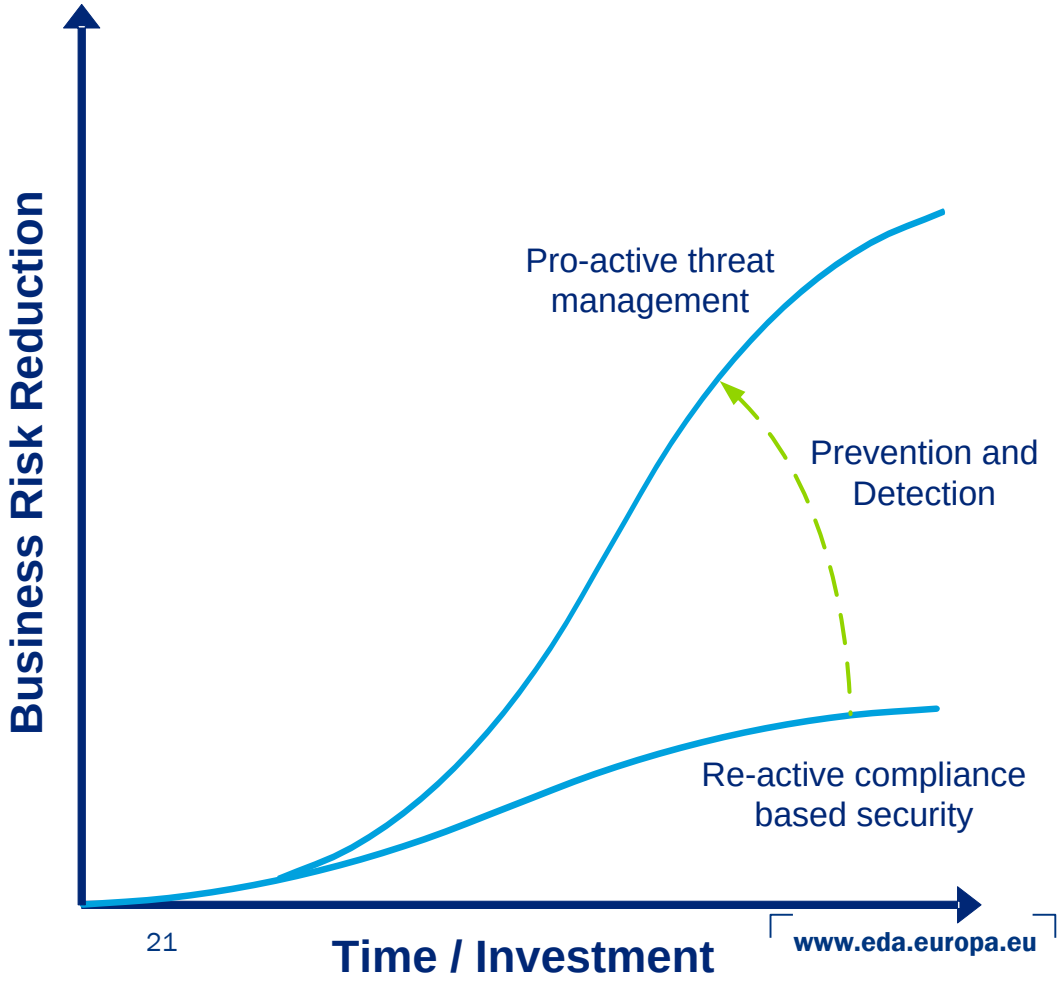


CyTeIOPS Project (2013) context

Move from information security to intelligent security

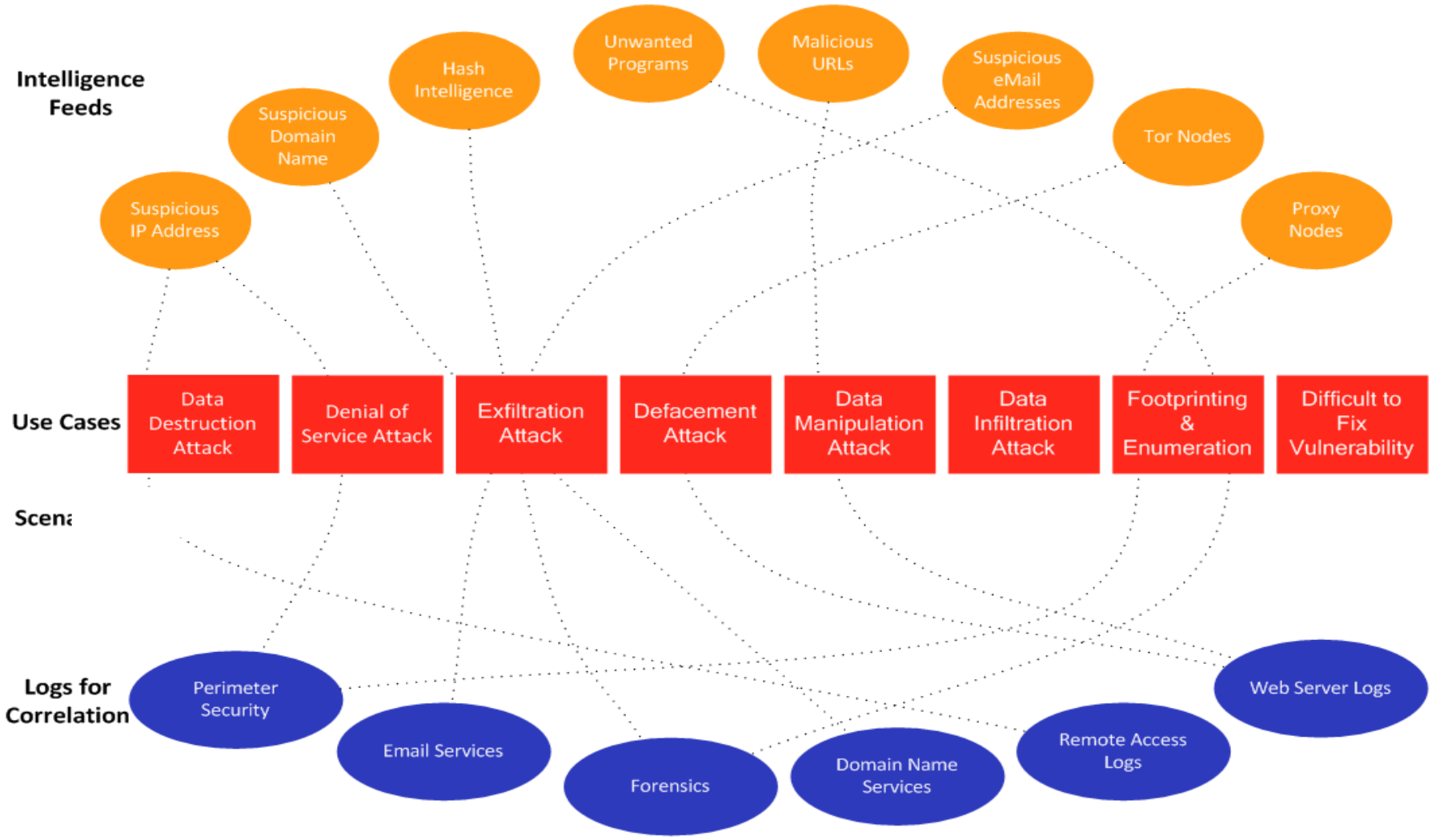
The new cyber threats require a new way of approaching security. To reduce risk, it is critical to be able to manage and monitor these threats effectively and pro-actively. This approach can be summarised by the following four key priorities:

- **Prepare:** prepare to defend against a targeted cyber attack, and to respond to an attack as it happens.
- **Aware:** identify and predict the targets and mechanisms of cyber attacks.
- **Respond:** be ready to respond to threat intelligence or an attack.
- Goal: move from a reactive posture based on compliance based security, to one that provides greater defence against targeted attacks, or greatly reduces their impact.

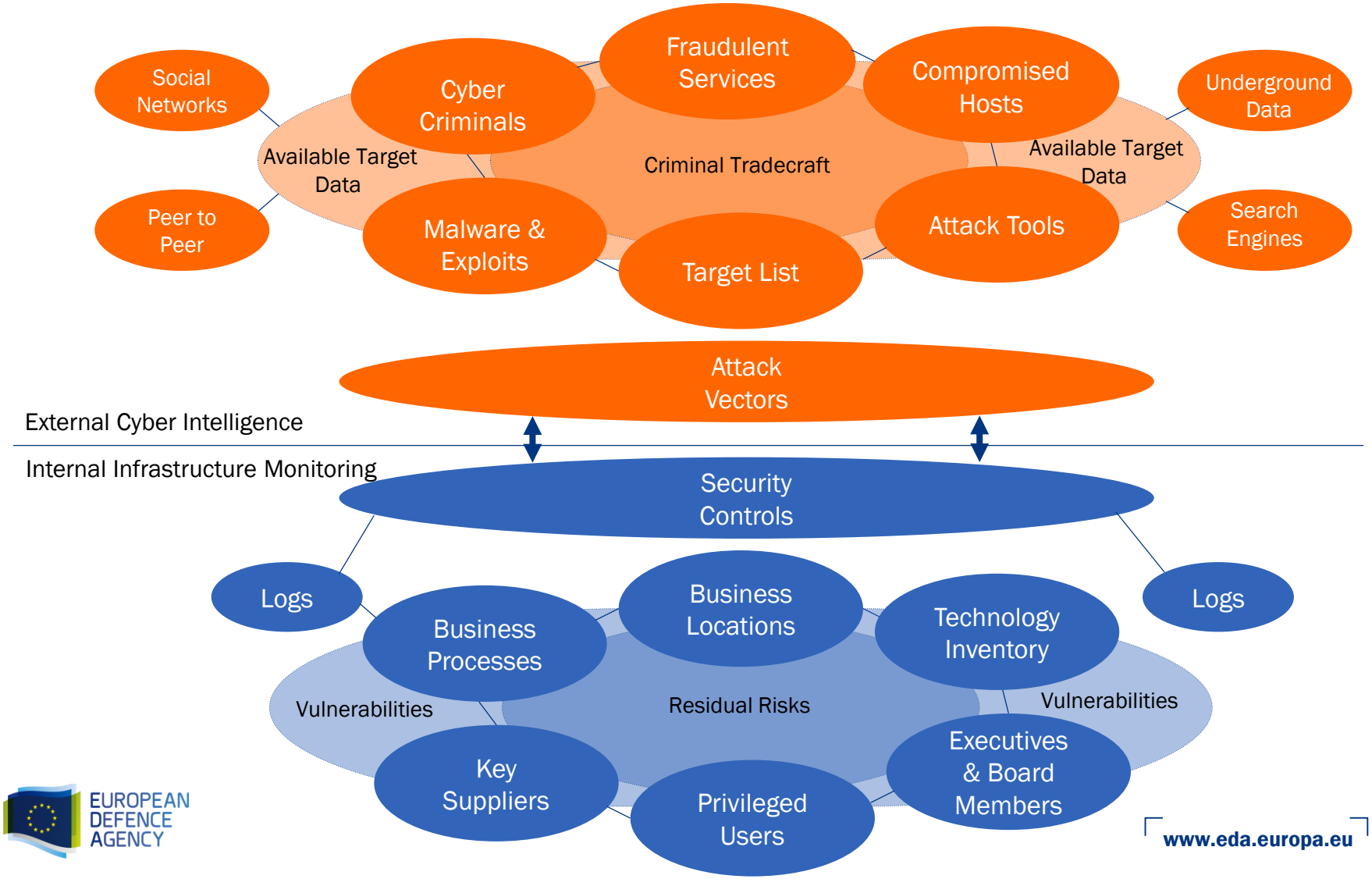


EUROPEAN DEFENCE AGENCY

Work Package 1 – Analysis of relevant cyber threat intelligence aspects of EU-led operations

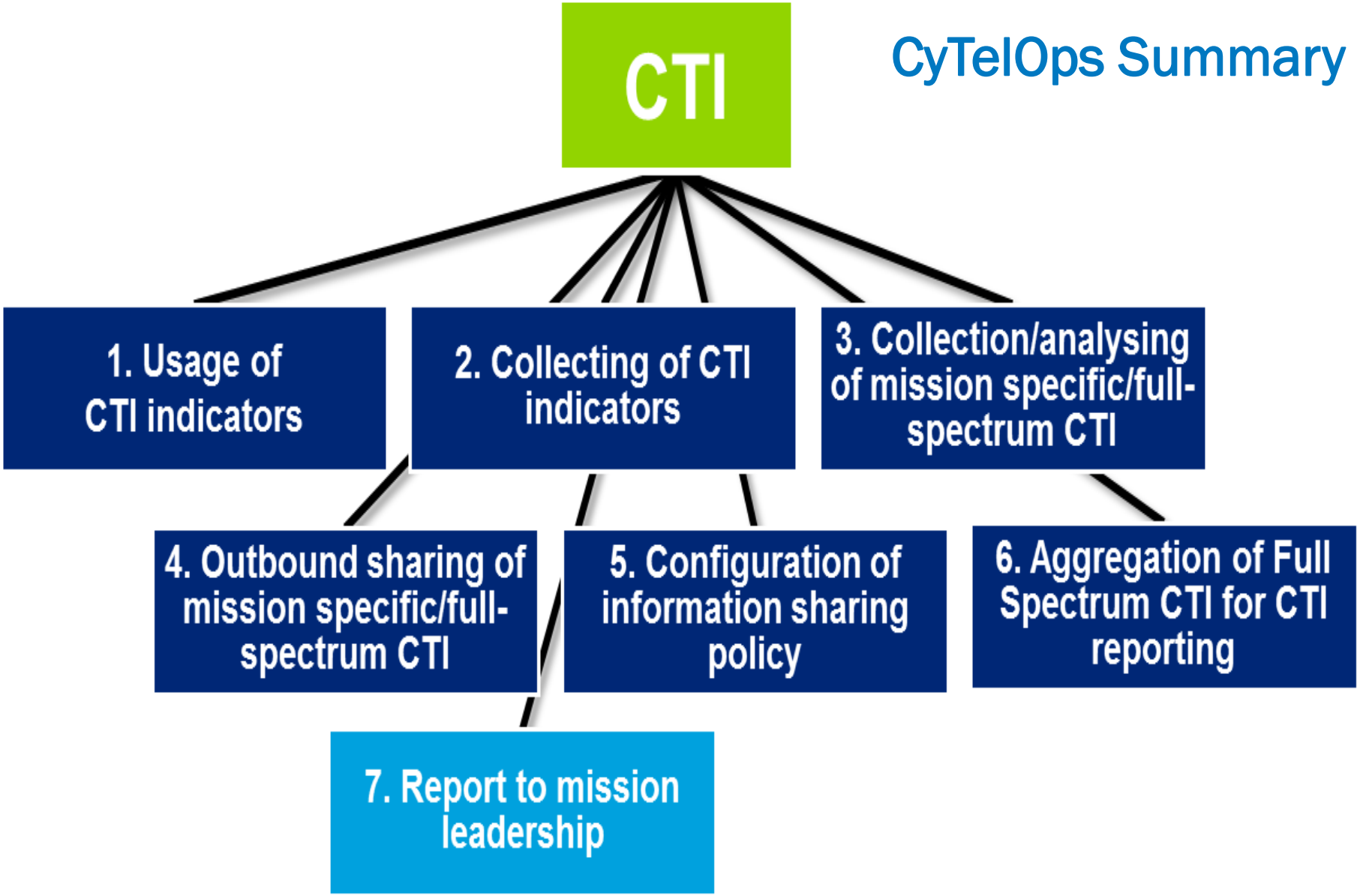


Work Package 2 – Identification and Modelling of Required Technology and Intelligence sources



EUROPEAN DEFENCE AGENCY

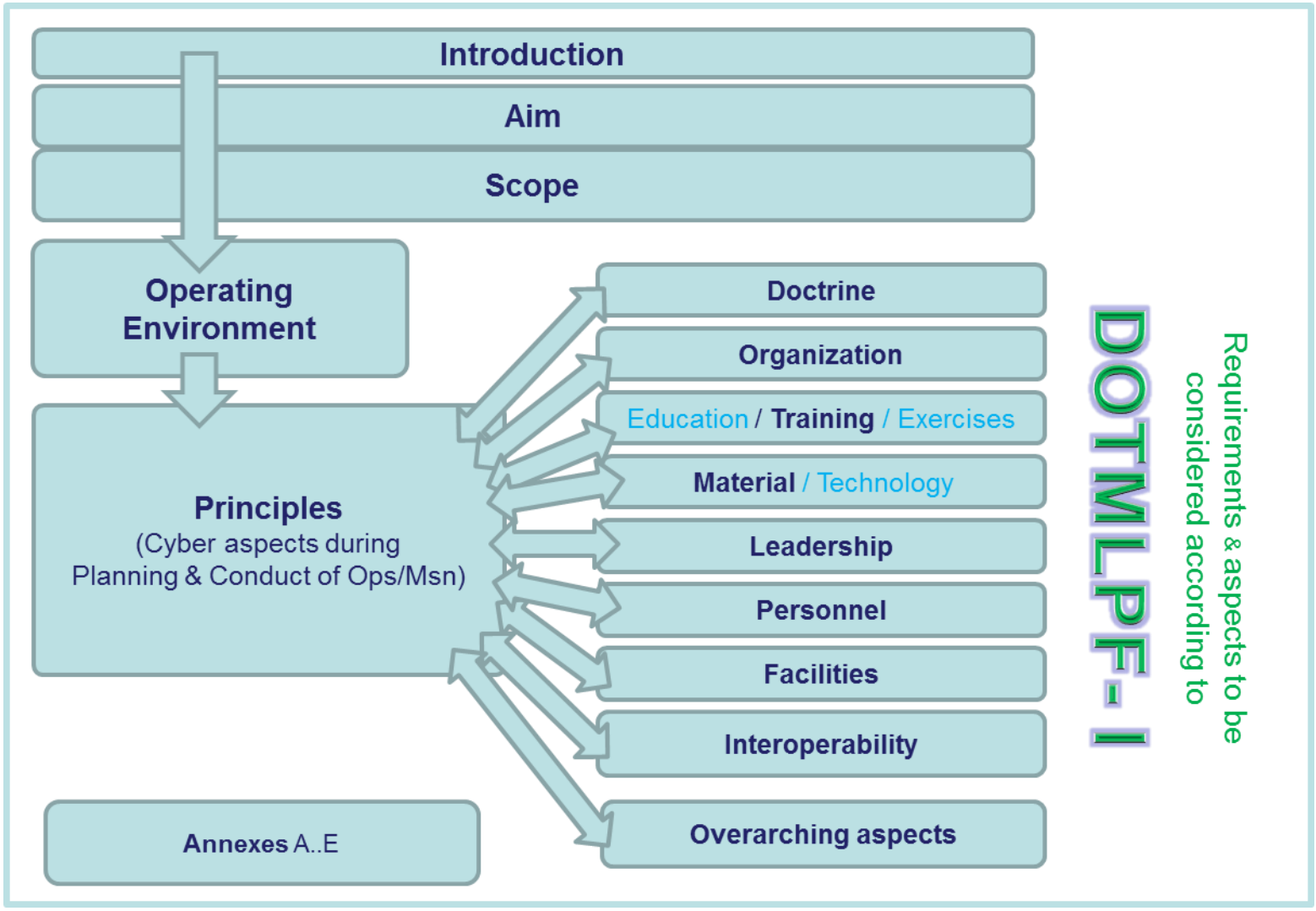
CyTelOps Summary



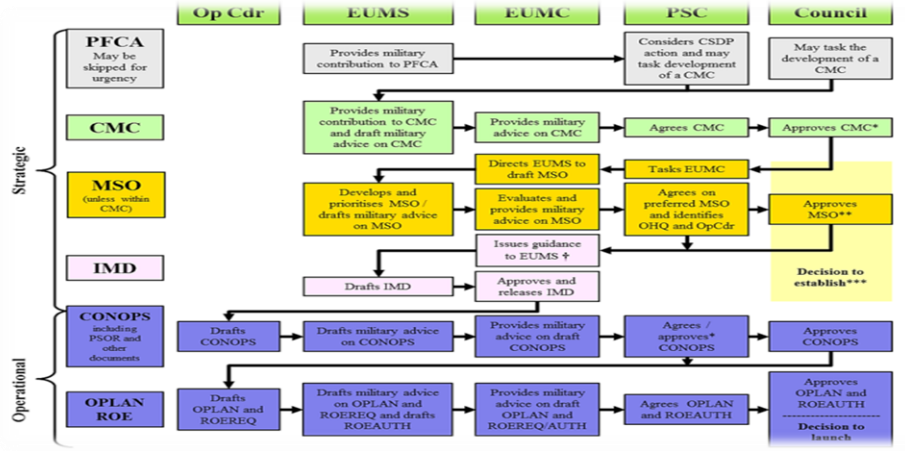
Talking Points

- EDA and Cyber Defence
- Cyber Defence and Cyber Threat Intelligence Considerations in the military Operations Planning Process
  - EDA „precursor“ work; Architecture and OPP
  - Cyber Situation Awareness;
  - CyTelOps
- The EU approach to Cyber Defences for EU-led Operations
  - The EU Cyber Defence Concept for military operations and missions
  - Considerations on Cyber Risk Management;
- Conclusions-Discussion Points

Cyber Defence Concept for EU-led military operations & missions

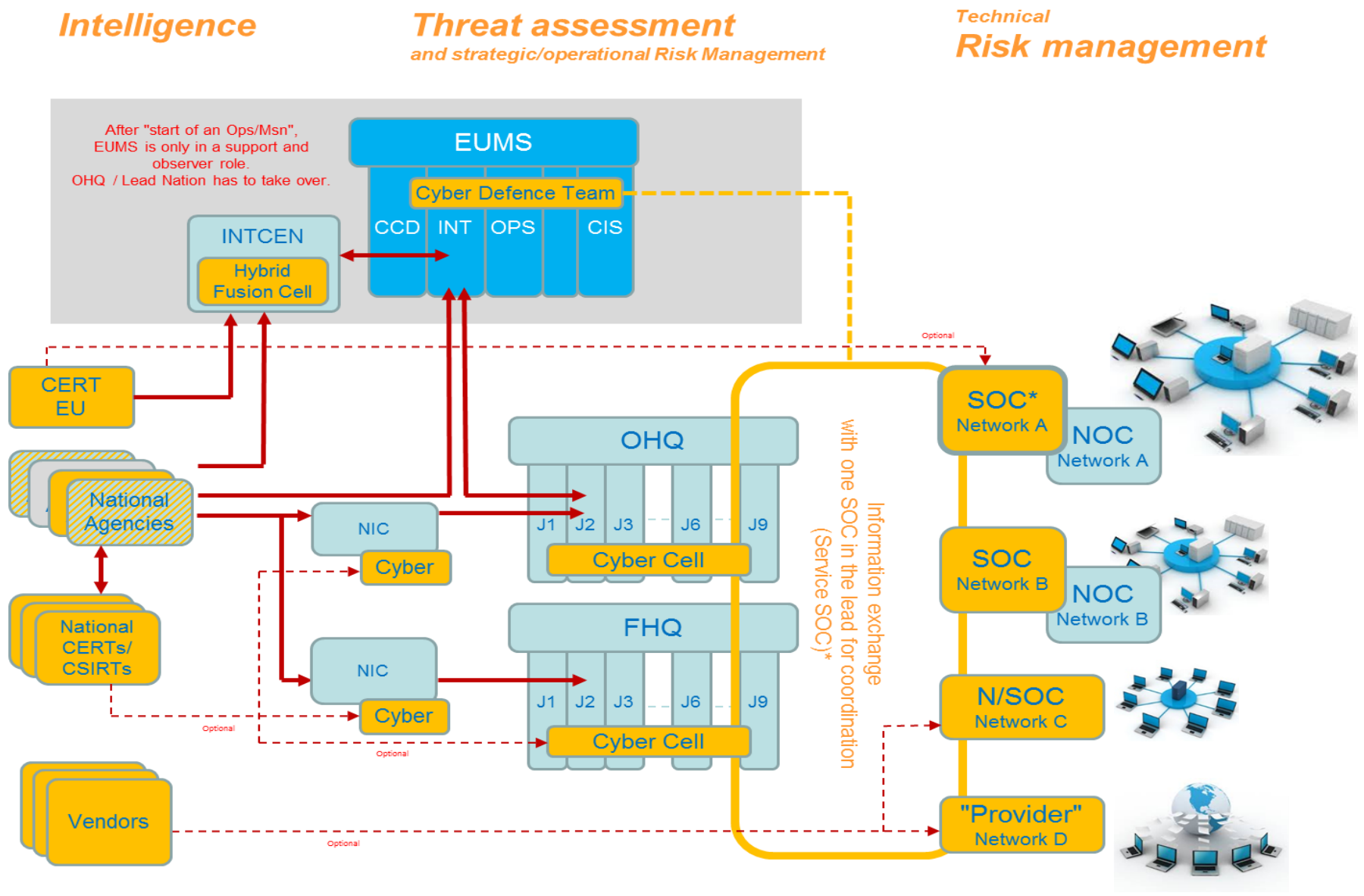


Cyber Defence Concept for EU-led military operations & missions ; Principles



- Planning…
  - "consider Cyber aspects as early as possible"
  - Cyber threat assessment supported by intelligence structures on request (cyber threat landscape)
  - EUMS to provide CD expertise into planning teams (for CMC and IMD)
  - Op/MsnCdr to consider CD in CONOPS and OPLAN, risk management by CIS/Cyber planners
  - Force generation and further planning (Cyber Service Catalogue, Cyber Cells in HQs)

Cyber Defence Concept for EU-led military operations & missions; Recommended Organisational Structure



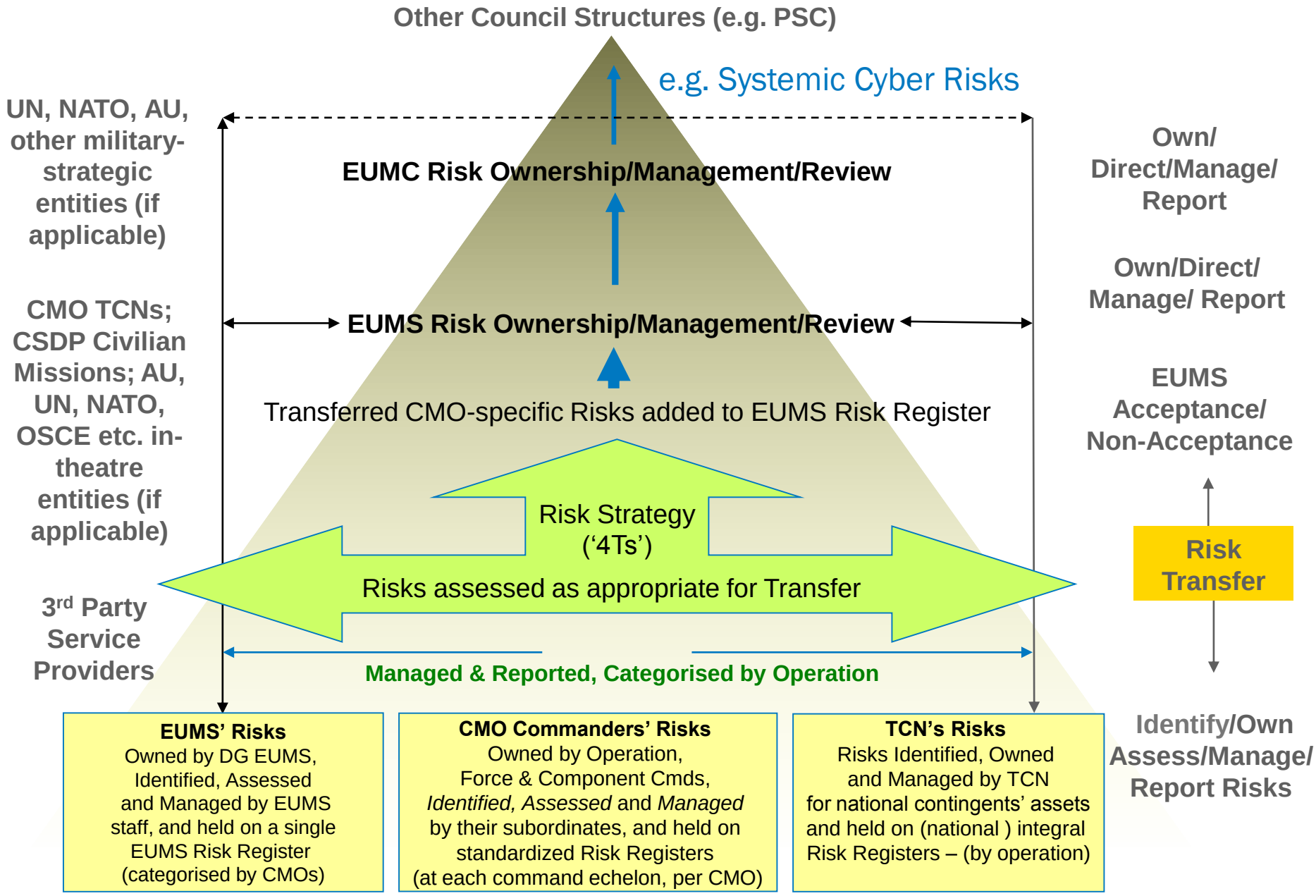
Dynamic Cyber Risk Management

- Risk is an equation of:
  - External and Internal **Threats** (external and internal Information/intelligence);
  - Own **Vulnerabilities in CIS** (internal information);
  - **Probability** of Occurrence (Dynamic Assessment);
  - Assessment of **Criticality** of CIS assets for business processes/mission success (Dynamic Assessment) ;
  - Business/Operations **Impact** (Dynamic Assessment) .
- Dynamic means not once but continuously
  - Fast moving threat landscape;
  - New vulnerabilities identified every day

  } requires a continuous flow of external and internal Information/intelligence).
- Risks are addressed via the 'Four Ts':

  Treat, Tolerate, Terminate, Transfer
  - Leadership decision;
  - Mitigation measures.
- Continuous Cyber Threat Intelligence is a key enabler for a viable Dynamic Cyber Risk Management.

Thoughts about a CSDP Cyber Risk Management and Escalation Process



Talking Points

- EDA and Cyber Defence
- Cyber Defence and Cyber Threat Intelligence Considerations in the military Operations Planning Process
  - EDA „precursor“ work; Architecture and OPP
  - Cyber Situation Awareness;
  - CyTelOps
- The EU approach to Cyber Defences for EU-led Operations
  - The EU Cyber Defence Concept for military operations and missions
  - Considerations on Cyber Risk Management;
- Conclusions-Discussion Points

Commander's key questions related to Cyber (source: CICOA)

1. How do regional and global actors with interests in the deployment region make use of the cyber domain (what are their offensive cyber capabilities, and what are their motivations and thresholds to employ offensive cyber capabilities)?
2. How can strategic cyber threats and cyber factors affect the operation?
3. Which options help to reduce undesirable consequences of cyber activities?
4. What is the applicable legal framework (e.g. Law of Armed Conflict) and which authorization (e.g. Rules of Engagement) and escalation processes are/have to be in place?
5. How do cyber factors affect own courses of action?
6. When and where are cyber-assets critical for success, what are their vulnerabilities and how can the risk that these vulnerabilities will be exploited be mitigated?
7. Which cyber defence considerations should be de-conflicted and coordinated with other considerations?
8. Which cyber defence activities should be synchronized with activities in other domains?
9. Who are relevant internal and external partners that can support in case of large scale incidents (e.g. CERT-EU, national CERTs, contracted service provider)?
10. Who should have the authority to release cyber defence related information to external partners?
11. What are the best mechanisms for optimal cyber information-sharing with external partners?
12. How should own cyber defence be organized (structure, manning, processes, disposition, equipment)?

Conclusion –Discussion Points

- The Threat Landscape becomes more and more diverse (e.g. hybrid);
- Cyber Threat Intelligence has to be integrated in the Military planning process from the earliest stage possible;
- Already conducted activities provide good input for the discussion in the military domain;
- Dynamic Risk Management and a continuous flow of cyber threat intelligence is key for success;
- Balanced set of competent personnel, state of the art technology and connecting processes (OPP, SOPs etc.) required;

"Is there any other business before we jump?"